

OT-CAP改善計畫

2026-01-12 14:00 - Joy Liao

| | | | |
|--|--------|--------|------------|
| 狀態: | New-新增 | 開始日期: | 2026-01-01 |
| 優先權: | Normal | 完成日期: | 2028-12-31 |
| 被分派者: | 君華 陳 | 完成百分比: | 0% |
| 分類: | | 預估工時: | 0:00 小時 |
| 版本: | | 耗用工時: | 0:00 小時 |
| 概述 CY-OT101 "OT - Roles and Responsibilities Entity level: Has a formal OT cybersecurity organization been defined and implemented with the appropriate correspondents across the entity? Site level: Has a local OT correspondent been identified for the site?" CY-OT102 "OT - Risk Management Has a risk analysis been conducted, validated by the business, and a budget allocated to deploy the appropriate action plan? " CY-OT103 "OT - Asset inventory Are all plant assets tracked in an asset inventory and kept up to date under the responsibility of the CISO with the support of the OT Correspondent? Is there a network diagram for the site?" CY-OT104 "OT - Sites/contracts inventory Are all contracts and plants listed with an identification of their criticality performed on a regularly basis at the entity level?" CY-OT105 "OT - Audit & Control Are there periodic audits and/or self-assessments based on the Fix the Basics including the supplier's managed perimeter? Are results shared to the relevant stakeholders (the Group, clients, etc.)? " CY-OT201 "OT - Awareness & Training Is there a dedicated industrial cybersecurity training in place for the OT cybersecurity team and is there an awareness program in place for OT Cybersecurity for plants' staff, visitors and suppliers?" CY-OT202 "OT - Security by design Is OT cybersecurity taken into account from end to end in projects with the involvement of the entity CISO or the local OT correspondent? " CY-OT203 "OT - Identity and access management Is there a documented and enforced process for access control, account management and access rights that takes into account the criticality of assets and user authorization ? " CY-OT205 "OT - Antivirus/EDR Is there an Antivirus/EDR deployed on the workstations and servers?" CY-OT206 "OT - USB protection Are USB keys sanitized before being connected to industrial workstations to avoid the introduction of malware within the ICS environment and disabled for non administrative usage?" CY-OT207 "OT - System hardening Is there an asset configuration hardening in place (workstations, servers, network equipments, PLCs)?" CY-OT208 "OT - Network security Does the network architecture of the industrial site respect the standard established by the group? " CY-OT209 "Vulnerability and patch management Is there a patch management process defined, documented and applied at plant level associated with a vulnerability management process to ensure related-risks are managed appropriately?" CY-OT210 "OT - Obsolescence Management Are obsolete assets formally tracked within the asset inventory? Is there an obsolescence remediation plan? " CY-OT301 "OT - Third-party management Are security requirements included and checked in tenders and contract with suppliers (incident handling, provision of security fixes, conditions for Remote Access or use of contractors' tools)?" CY-OT302 "OT - Remote Access Do you have a secure remote access process?" CY-OT401 "OT - Detection - Logging & Monitoring Are event logs with relevant security information (source, date, user and timestamps) implemented on the systems that support them ? Are these logs collected into a SIEM and analyzed by a SOC? | | | |

| | | |
|--|--|--------|
| " | | |
| CY-OT402 "OT - Incident & Crisis Management | | |
| Is there an incident management plan, including reporting of incident to local CISO and Group Cybersecurity, and a crisis management plan, including cybersecurity event scenarios, documented?" | | |
| CY-OT501 "OT - Backup & Restore | | |
| Is there a documented and implemented backup management procedure that takes into account the complete backup of industrial equipment, recovery tests, offline data storage and business data retention ?" | | |
| CY-OT502 "OT - BCP | | |
| Is there a BCP/DRP documentation and processes in place that include industrial cybersecurity aspects? | | |
| Have degraded modes been identified/tested with the business in case of cyberattack and is an OT systems rebuild procedure formalized/tested?" | | |
| 子任務: | | |
| 資安改善 # 1334: CY-OT101 | | New-新增 |
| 資安改善 # 1335: CY-OT102 | | New-新增 |
| 資安改善 # 1336: CY-OT103 | | New-新增 |
| 資安改善 # 1337: CY-OT104 | | New-新增 |
| 資安改善 # 1338: CY-OT105 | | New-新增 |
| 資安改善 # 1339: CY-OT201 | | New-新增 |
| 資安改善 # 1340: CY-OT202 | | New-新增 |
| 資安改善 # 1341: CY-OT203 | | New-新增 |
| 資安改善 # 1342: CY-OT205 | | New-新增 |
| 資安改善 # 1343: CY-OT206 | | New-新增 |
| 資安改善 # 1344: CY-OT207 | | New-新增 |
| 資安改善 # 1345: CY-OT208 | | New-新增 |
| 資安改善 # 1346: CY-OT209 | | New-新增 |
| 資安改善 # 1347: CY-OT210 | | New-新增 |
| 資安改善 # 1348: CY-OT301 | | New-新增 |
| 資安改善 # 1349: CY-OT302 | | New-新增 |
| 資安改善 # 1350: CY-OT401 | | New-新增 |
| 資安改善 # 1351: CY-OT402 | | New-新增 |
| 資安改善 # 1352: CY-OT501 | | New-新增 |
| 資安改善 # 1353: CY-OT502 | | New-新增 |

歷史

#1 - 2026-01-12 14:10 - Joy Liao

- 子任務 #1334 已新增

#2 - 2026-01-12 14:10 - Joy Liao

- 子任務 #1335 已新增

#3 - 2026-01-12 14:10 - Joy Liao

- 子任務 #1336 已新增

#4 - 2026-01-12 14:11 - Joy Liao

- 子任務 #1337 已新增

#5 - 2026-01-12 14:11 - Joy Liao

- 子任務 #1338 已新增

#6 - 2026-01-12 14:11 - Joy Liao

- 子任務 #1339 已新增

#7 - 2026-01-12 14:11 - Joy Liao

- 子任務 #1340 已新增

#8 - 2026-01-12 14:12 - Joy Liao

- 子任務 #1341 已新增

#9 - 2026-01-12 14:12 - Joy Liao

- 子任務 #1342 已新增

#10 - 2026-01-12 14:12 - Joy Liao

- 子任務 #1343 已新增

#11 - 2026-01-12 14:12 - Joy Liao

- 子任務 #1344 已新增

#12 - 2026-01-12 14:13 - Joy Liao

- 子任務 #1345 已新增

#13 - 2026-01-12 14:13 - Joy Liao

- 子任務 #1346 已新增

#14 - 2026-01-12 14:13 - Joy Liao

- 子任務 #1347 已新增

#15 - 2026-01-12 14:13 - Joy Liao

- 子任務 #1348 已新增

#16 - 2026-01-12 14:13 - Joy Liao

- 子任務 #1349 已新增

#17 - 2026-01-12 14:14 - Joy Liao

- 子任務 #1350 已新增

#18 - 2026-01-12 14:14 - Joy Liao

- 子任務 #1351 已新增

#19 - 2026-01-12 14:14 - Joy Liao

- 子任務 #1352 已新增

#20 - 2026-01-12 14:14 - Joy Liao

- 子任務 #1353 已新增

#21 - 2026-01-12 14:22 - Joy Liao

- 被分派者 設定為 君華 陳